

ATTACHMENT B

Information and Evidence to be Seized

1. Global Positioning System (GPS) data indicating the location of the **Target Cellular Device**;
2. Digital photographs or video files depicting firearms or ammunition, or that relate to the sale or purchase of a firearm or ammunition;
3. Lists, ledgers, records, notes, spreadsheets, or similar files documenting the possession or sale of firearms or ammunition and/or identifying individuals involved in those transactions;
4. Electronic communications including email, text messages, multimedia messages, and communications through social media networks and applications relating to firearms or ammunition possession, purchase, and transfer;
5. Toll records documenting incoming and outgoing phone calls, text messages, and email;
6. Audio files including voice mail messages or chats relating to firearms or ammunition possession or transfer;
7. Evidence of user attribution showing who used or owned the **Target Cellular Device** at the time items and records described in this warrant were created, edited, or deleted, such as phone calls, internet searches, photos and videos;
8. Contact lists;
9. Bank records, including electronic copies or photographs of checks, deposit slips, account statements, wire transfer documentation, documentation of electronic money transmissions through money transfer businesses to include Western Union and MoneyGram, and credit card account statements;
10. Records of things evidencing the use of the internet, including;
 - a. Records of Internet Protocol (IP) addresses used; and
 - b. Records of internet activity, including firewall logs, caches, browser history and cookies, bookmarked or favorite webpages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.